The Industrial Control System Cyber Defence Triage Process

Allan Cook, Helge Janicke, Richard Smith, Leandros Maglaras

Cyber Technology Institute, De Montfort University, Leicester, LE1 9BH, UK

Abstract

The threat to Industrial Control Systems (ICS) from cyber attacks is widely acknowledged by governments and literature. Operators of ICS are looking to address these threats in an effective and cost-sensitive manner that does not expose their operations to additional risks through invasive testing. Whilst existing standards and guidelines offer comprehensive advice for reviewing the security of ICS infrastructure, resource and time limitations can lead to incomplete assessments or undesirably long countermeasure implementation schedules.

In this paper we consider the problem of undertaking efficient cyber security risk assessments and implementing mitigations in large, established ICS operations for which a full security review cannot be implemented on a constrained timescale. The contribution is the Industrial Control System Cyber Defence Triage Process (ICS-CDTP). ICS-CDTP determines areas of priority where the impact of attacks is greatest, and where initial investment reduces the organisation's overall exposure swiftly. ICS-CDTP is designed to be a precursor to a wider, holistic review across the operation following established security management approaches. ICS-CDTP is a novel combination of the Diamond Model of Intrusion Detection, the Mandiant Attack Lifecycle, and the CARVER Matrix, allowing for an effective triage of attack vectors and likely targets for a capable antagonist. ICS-CDTP identifies and focuses on key ICS processes and their exposure to cyber threats with the view to maintain critical operations. The article defines ICS-CDTP and exemplifies its application using a fictitious water treatment facility, and explains its evaluation as part of a large-scale serious game exercise.

Keywords: ICS, SCADA, cyber, security, triage, risk

1. Introduction

Modern Industrial Control Systems (ICS) have evolved from isolated environments that traditionally had no external connectivity to integrated architectures. This integration is business driven, with the objective to exploit the value of operational data to maximise efficiencies and streamline supply chains. Most ICS systems are optimised for performance, and were historically not designed to defend against unauthorised or malicious use. Typical ICS architectures comprise a mix of operational technologies (OT) that include field measurement and control devices integrated with established information technology (IT) supervisory applications. OT is often based on proprietary hardware and protocols, complicating risk assessments and the development and deployment of counter measures. ICS are deterministic real-time systems that operate within strict latency boundaries to ensure operation of critical industrial processes found in chemical processing or power generation. Once installed and certified for safety compliance, these systems are rarely updated, as the risk of unexpected behaviours as a result of modification is perceived as high and testing on dedicated off-line facilities is prohibitively expensive. As a consequence the deployed devices often remain in operation for 10-20 years with little modification [1, 2, 3, 4]. Regular security or functional updates that are common to the modern IT are not commonly deployed in these infrastructures making them exceptional vulnerable to attack. The maintenance of availability, reliability and safety of an ICS is a priority, and any downtime to install upgrades, patches, or add security features that may assist in the response to a cyber incident, are uncommon [5, 6].

There is evidence [7, 8] that targeted attacks from capable actors look beyond a IT system focus, and instead target directly the industrial processes under control in order to create an effect that impacts on the operations of an industrial facility. This attack on the critical processes represents the highest level of threat to an ICS operator, especially when perpetrated by a highly capable actor such as a nation state [9]. Any approach to security of ICS hence should assume an intelligent, adaptable adversary that will focus on high-value targets.

Traditional approaches to systems vulnerability assessment rarely focus on antagonistic intent. Instead they review penetration and exploitation options, highlighting what is vulnerable as a result. A complete review of a facility using the guidance in ISA-99 [10], soon to be replaced by IEC

62443 [11], and the CPNI ICS Good Practice Guide [12] should result in a comprehensive defence-in-depth approach to cyber security. However, such comprehensive reviews are expensive, resource-intensive activities that often cannot be justified purely based on a cost-benefit analysis.

In order to deliver the maximum return on investment for an initial cyber review, and establish the basis for a subsequent complete assessment of the operations, the potential financial and safety impacts of malicious attack activity should be modelled to determine where the manipulation of industrial processes and process data have the greatest impact. It is only once the process vulnerabilities in the operational industrial processes have been identified that we can establish which of the many devices within a large ICS installation are responsible for the control of the vulnerable process steps, and triage which are the highest priority to defend from cyber attack, and against which we can build an incident response 'playbook' to deny the attacker access to critical system assets.

Whilst the total global automation market in 2012 was estimated to be worth USD 152bn [13], the US ICS-CERT only responded to 138 incidents [14]. Between October 2014 and September 2015 the number of incidents had increased to 295 [15], but compared to the global value of the market, and the inferred number of ICS installations worldwide, the frequency of incidents remains low.

This relative infrequency is not proportionate to the potential impact. A simulation of malware on the US electricity grid [16] resulted in blackouts across 15 states, 93 million people without power, and impacts on the US economy of between USD 243bn and 1trn. Such high-impact, low-frequency (HILF) events [17] do not provide an adequate dataset to characterise the threat and do not provide sufficient inputs to established risk analysis models [18]. This lack of evidence complicates the cost-justification of investment in ICS cyber security, as the costs can be high versus the demonstrated number of incidents.

The ICS-CDTP framework described within this paper is focused on those ICS operators facing the highest levels of impact from antagonistic cyber actions, but are not yet at a high level of cyber security maturity. The intent of ICS-CDTP is to *begin* a progression of informing and realising a set of ICS security controls that will form the basis of subsequent, holistic analyses of the entire industrial facility using established best practices.

ICS-CDTP framework is novel in that it combines and extends concepts found in risk assessment and intrusion detection techniques with safety and

process models that are known within the operations of many ICS facilities. As such, ICS-CDTP:

1. Focuses on the identification and defence of critical ICS equipment from malicious manipulation. It models and characterises attack behaviours and support the development of a set of potential intrusion models that significantly improve the readiness of incident responders.
2. Is intended to be complementary to IEC 62443 [11] and the CPNI ICS Good Practice Guide [12]. It extends the Diamond Model of Intrusion Analysis [19] and integrates the CARVER Matrix [20] to support a fundamental change from reactionary, blanket protection to targeted and focussed defence.
3. Allows ICS operators to actively identify and attempt to thwart malicious attacks based on an incident response 'playbook' developed from analyses of antagonistic intent.

The remainder of this article is structured as follows:
ICS-CDTP Framework: We introduce ICS-CDTP and review how we characterise the attractiveness of a target to an antagonist, and which questions we must ask as a consequence to better inform incident response planning.
ICS-Cyber Defence Triage Process: We explain the stages of the ICS-CDTP in detail, articulating how we integrate the Mandiant Attack Lifecycle with the Diamond Model of Intrusion Detection, and how we extend the Diamond Model to accommodate ICS equipment. We then proceed to explain the CARVER Matrix as a method to triage critical systems, and show how ICS-CDTP leverages a modified version of the CARVER Matrix to prioritise which systems require an immediate focus for cyber defensive actions. We proceed to illustrate how to address the protection of systems identified as critical, and support the development of an incident response 'playbook'.
Evaluation: We explain how we have evaluated ICS-CDTP sufficiently to demonstrate the feasibility of the framework to be taken forward to testing on a large-scale, production ICS.
Conclusions: We discuss the evaluation, considering the limitations of the testing environment to date, and propose future steps to develop ICS-CDTP into a viable, cost-effective triage mechanism for ICS.

2. The ICS-CDTP Framework

To date, there has been a lack of validated data against which we can apply established risk models to ICS cyber threats [21, 18]. The ICS-CDTP framework assumes that the courses of action an adversary will pursue when attacking an ICS are unknown to the defender. Whilst some opportunist antagonists may attempt to cause disruption without any conscious targets, highly capable attacks will develop elaborate and coordinated attacks against the highest value targets. By assuming a highly capable attacker the ICS-CDTP framework considers a worst-case scenario driving the risk assessment.

Regardless of the premeditation of an attacker, an assessment of which systems are critical to the continued operation of an industrial facility is required. This includes the assessment of the vulnerabilities of the specific control devices used and the infrastructure that underpins them with the aim to establish *attractive* targets.

ICS-CDTP defines an *attractive* target as one that is: *i)* poorly protected, either through inherent flaws in the device or weaknesses in surrounding security mechanisms, *ii)* critical to the correct and profitable execution of an operational process, *iii)* used in processes that, if manipulated, would result in the local population or general public becoming aware of the intrusion, *iv)* easily accessible via Internet-enabled devices, or poorly protected from insiders through inadequate physical security. These characteristics focus on the adversary's perspective of the ICS infrastructure, and their attack intent. Targets that satisfy these criteria would offer a means by which a capable antagonist could achieve significant impact on an ICS [9].

ICS-CDTP (Fig.1), iteratively assesses the attractiveness of a device to an antagonistic actor and provides a process to remediate any vulnerabilities, as well as describing any residual risk and informing security monitoring techniques for mitigation. However, analysis alone is not sufficient to adequately defend an ICS, it must also support ongoing security monitoring to better identify intrusions and underpin subsequent incident response. As a result, this framework addresses eight questions:

1. Which devices are attractive to an attacker?
2. Can we better protect these devices?
3. What routes exist to these devices?
4. What events would occur in an attempt to access and manipulate these devices?
5. Where can we deploy sensors to detect these events?

6. How will we determine which of the alternate routes to a device are being used by an attacker?
7. How can we predict an attackers next activity?
8. What does our incident response plan need to describe and test in order to mitigate residual risks identified in the analysis?

3. ICS Cyber Defence Triage Process

The scale of ICS installations often complicates the cyber security analysis process, as it is not cost-effective to defend all systems equally in such a complex environment. Given the number of devices installed it is desirable to prioritise the defence of those that support critical functionality. This should include assessments from both offensive and defensive perspectives. Fig. 1 describes the ICS Cyber Defence Triage Process.

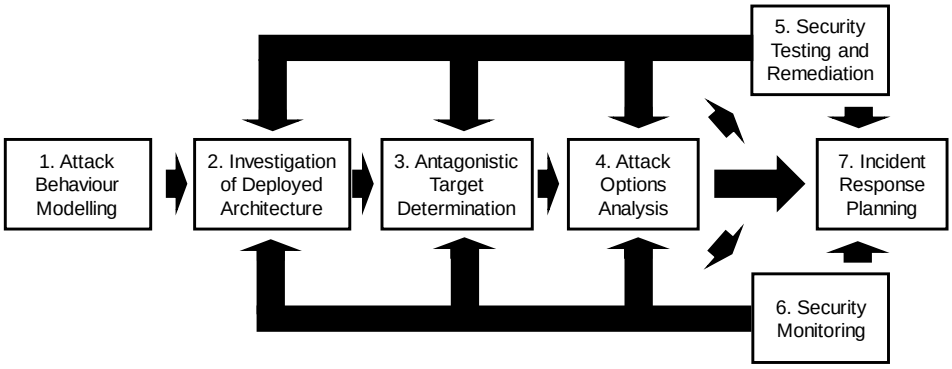

Figure 1: ICS Cyber Defence Triage Process (ICS-CDTP)

Capable threat actors tend to follow established Advanced Persistent Threat (APT) approaches to targets [22]. In 2014, 55 percent of incidents investigated by ICS-CERT involved APTs or sophisticated actors [15]. In order to maintain a focus on such antagonists we must first decide how to represent the behaviours of an attacker. The triage framework illustrated in Fig. 1 begins in Step 1 by deciding upon an attack lifecycle model that best suits the perceived threat and available data. It then proceeds to gather documentation on the ICS network architecture in Step 2. Whilst information obtained from network enumeration is always more accurate, ICS devices are

known to react unpredictably to such exercises, and this will expose the operations of the facility to unnecessary risk. The network design documentation is then used as a foundation for all subsequent analysis.

At this point, in Step 3, an assessment is made regarding the impact and attractiveness of key processes to an antagonist, and the underlying ICS devices, followed by a review of the possible attack threads that could permit access to the ICS in Step 4. These attacker courses of action will, however, be constrained by the characteristics of the ICS architecture implemented within the facility. Accordingly, we consider the deployed infrastructure of the facility to increase the specificity of the analysis. By combining and analysing the critical devices, attacker behaviours, and the deployed ICS architecture, we produce a triage of the options available to an antagonist. This drives the detailed security analysis of the critical devices in Step 5, either leading to remediation of vulnerabilities, or where this is not possible, the identification of indicators of compromise and the locations where network- and host-based sensors can be deployed to support targeted security monitoring in Step 6. Both options should feed into the overall incident response planning process of Step 7, to underpin effective cyber defences against malicious attacks.

We will now consider each of the triage framework steps in greater detail.

The first step of the proposed framework defines how the antagonist's behaviour will be described, as a basis for subsequent analysis, by extending the Diamond Model of Intrusion Analysis [19] and integrating it with the Mandiant Attack Lifecycle [22, 23]. The Diamond Model [19] is an analysis framework that defines atomic intrusion events and describes the four core features of an antagonistic event, those being an *adversary* using a *capability* delivered over an *infrastructure* in order to target a *victim* and produce an outcome (Fig. 2). These core features, or nodes, are connected by edges that define the relationship between each. The nodes and edges are connected into a model that resembles a diamond. The event also has a number of meta-features that allow further details of an intrusion event to be modelled. All attributes have an associated confidence level to allow a weighting to be applied to decisions taken on the perceived accuracy of data. The advantage of the model comes from the ability to analytically pivot between the connected points on the diamond to reach other connected points, allowing, for example, common capabilities being used in different intrusion events.

Rather than being defined as a specific ontology or taxonomy for modelling attack behaviours, the diamond model is intended to be an extendable framework that can accommodate architectures and technologies as befits an

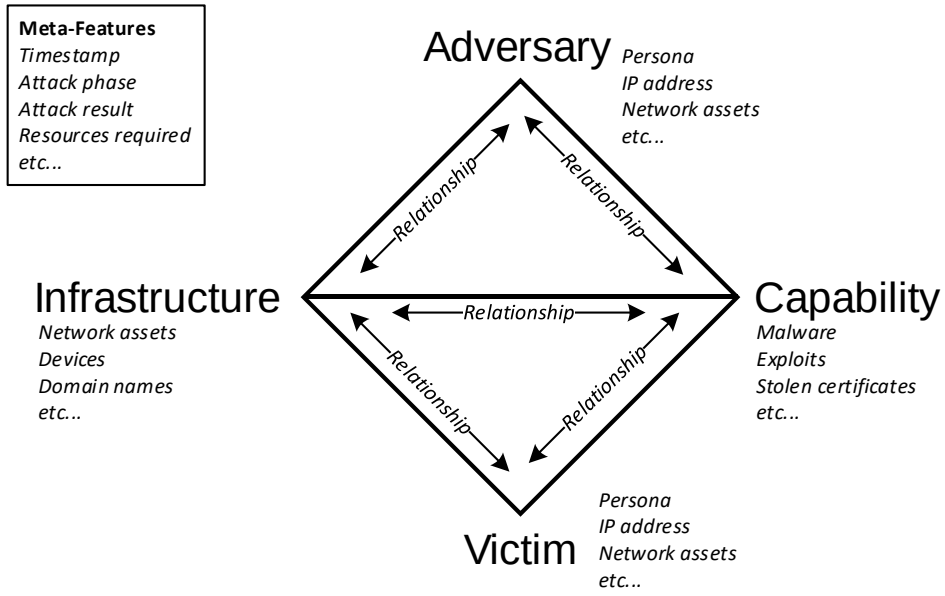

Figure 2: Diamond Model [19]

environment. As a result, an event in the model is a variable-sized n-tuple that allows a basic tuple to be extended based on requirements.

The basic diamond event, along with the standard victim definition, is depicted in Fig. 3.

There are many ways to express an antagonistic cyber attack. Two commercial methods were considered during this analysis; the Lockheed Martin 'Kill-Chain' [24] and the Mandiant Attack Lifecycle [22, 23]. Both techniques fitted within the process, but in this example we used the Mandiant method, as the 'Weaponisation' phase of the Lockheed Martin model would be opaque to a defender. The Mandiant lifecycle comprises eight stages:

1. External Reconnaissance: *Network scanning and associated research into the target organisation and systems.*

2. Initial Compromise: *The methods by which an attacker passes the security perimeter of the target network.*

3. Establish Foothold: *Techniques and capabilities to establish two-way communications with implanted malware.*

$$
\begin{aligned}
E = \langle\langle & \text{Adversary, Confidence}_{adversary}\rangle \\
& \langle \text{Capability, Confidence}_{capability}\rangle \\
& \langle \text{Infrastructure, Confidence}_{infrastructure}\rangle \\
& \langle \text{Victim, Confidence}_{victim}\rangle \\
& \langle \text{Timestamp-Start, Confidence}_{timestamp\text{-}start}\rangle \\
& \langle \text{Timestamp-End, Confidence}_{timestamp\text{-}end}\rangle \\
& \langle \text{Phase, Confidence}_{phase}\rangle \\
& \langle \text{Result, Confidence}_{result}\rangle \\
& \langle \text{Direction, Confidence}_{direction}\rangle \\
& \langle \text{Methodology, Confidence}_{methodology}\rangle \\
& \langle \text{Resources, Confidence}_{resources}\rangle\rangle
\end{aligned}
$$

$$
\begin{aligned}
\langle \text{Victim, Confidence}_{victim}\rangle = & \\
& \langle \text{Organisation, Confidence}_{organisation}\rangle \\
& \langle \text{HostIPAddress, Confidence}_{IP}\rangle \\
& \langle \text{Hostname, Confidence}_{hostname}\rangle \\
& \langle \text{Application, Confidence}_{application}\rangle \\
& \langle \text{TCPPort, Confidence}_{TCPport}\rangle\rangle
\end{aligned}
$$

Figure 3: Basic Diamond Event and Standard Victim Definition[19]

4. Escalate Privileges: *The means by which an attacker elevates their permissions to a greater set of resources.*
5. Internal Reconnaissance: *Scanning and device discovery within the target network.*
6. Move Laterally: *Traversion of the target network across legitimate devices.*
7. Maintain Presence: *Ensuring continued control over key systems, nodes and devices.*
8. Complete Mission: *The execution of the intent of the attack.*

The lifecycle offers the ability to model the attack methods of an antagonist in a uniform manner to allow an assessment of behaviours towards the intended target devices. However, in order to consider the feasibility of these

attacker options we must also take into account the deployed architecture of the ICS under analysis.

Security can be reduced through poor systems integration or inadequate control over communications. As a result, the ICS devices cannot be considered in isolation from the network on which they are deployed. The second step of the proposed framework investigates this deployed architecture. Whichever way the architecture has been defined within the ICS operation, whether that be through layering, grouping, functional separation etc., it must feature in the triage framework so that we can review its impact and determine common vulnerabilities that arise as a consequence of the design. ICS are typically not deployed in a consistent manner, and therefore the triage framework does not prescribe any defined abstractions. However, for the purposes of explaining the triage process, we shall us the Purdue Model of Control Hierarchy [25] as an illustrative architecture.

The Purdue model, a reference architecture for control hierarchy [25] that describes six levels within an organisation managing an industrial control system (Fig. 4). ICS implementations often include a number of significant differences to traditional IT systems. Typically, ICS have a deeper architecture than typical enterprises, as characterised by the Purdue model.

In order to accommodate the idiosyncrasies of ICS into the process we must extend the definition of an event within the Diamond Model. Whilst no mandatory elements are prescribed in the model, the *infrastructure* and *victim* nodes should include the following levels of granularity to support a detailed analysis of attack options.

Input Protocol: The protocol used to access the device.
Input Bearer: The bearer over which the input protocol runs, in order to determine if it is shared.
Output Protocol: The protocol exiting the device, to accommodate protocol transformations.
Output Bearer: The bearer over which the output protocol runs, in order to determine if it is shared.
Network Segment / Identifier: Which network or bus segment, or serial identifier, is used to over the bearers.
Architecture Layer: Which layer or zone the segment sits within.
Target Device: The make and model of the device.
Target Device Address: Its address, whether IP, MAC or otherwise.
Target Device Port / Identifier: What port, or other identifier is used to communicate with the device.

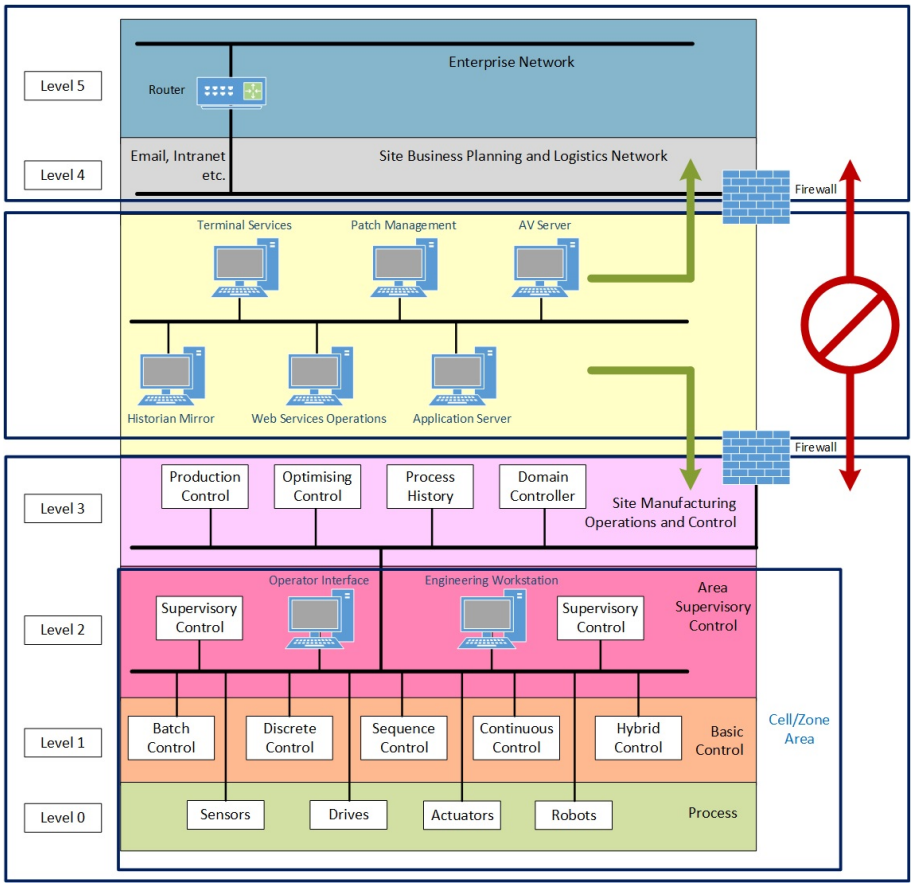

Figure 4: Purdue Model for Control Hierarchy[25]

Hardware Revision: The hardware revision of the device.
Firmware Revision: The firmware revision of the device.
OS Revision: The operating system revision of the device.
Process: Which process the device is used within.
Process Step: Which specific step of the process.
Process Impact: The impact, potential or real, of manipulating the device.
Loss: The associated, assessed financial loss through manipulation.

Extensions to the Infrastructure and Victim nodes are represented in Fig. 5.

The Diamond Model then needs to be integrated with the selected attack lifecycle (or *'kill-chain'*), in this case the Mandiant Attack Lifecycle [22].

Fig. 6 shows a set of Activity Threads [19] with intrusion events modelled

$<Victim, Confidence_{victim}> =$
$<<TargetDevice, Confidence_{tgtdevice}>$
$<TargetDeviceAddress, Confidence_{tgtdevaddress}>$
$<TargetDevicePort/Identifier, Confidence_{tgtdevID}>$
$<HardwareRevision, Confidence_{HWrevision}>$
$<FirmwareRevision, Confidence_{SWrevision}>$
$<OSRevision, Confidence_{OSrevision}>$
$<Process, Confidence_{process}>$
$<ProcessStep, Confidence_{processstep}>$
$<ProcessImpact, Confidence_{processimpact}>$
$<Loss, Confidence_{loss}>>$

$<Infrastructure, Confidence_{infrastructure}> =$
$<<InputProtocol, Confidence_{inputprotocol}>$
$<InputBearer, Confidence_{inputbearer}>$
$<OutputProtocol, Confidence_{outputprotocol}>$
$<OutputBearer, Confidence_{outputbearer}>$
$<NetworkSegment/Identifier, Confidence_{segment}>$
$<ArchitectureLayer, Confidence_{architecturelayer}>>$

Figure 5: Extensions to the Definition of Victim Infrastructure Nodes

as diamonds. Activity Threads, however, lend themselves more to intrusion analysis activities, whereas we require a mechanism to develop attack routes prior to the event, in order to develop our understanding of potential attack paths.

Fig. 7 uses Activity Threads from a single adversary to model the various options available to attack a victim device. The resulting Activity-Attack Graph allows the various possible routes to the target, and the associated events, to be modelled. The graph models, in a simple format, the alternative paths that can be considered when assessing how to defend the target device. It drives the definition of sensor and log alerts to inform on such behaviour. Should an intrusion occur, the analysis is already mature as a consequence of these models, and attacker next steps can be considered.

The third step of the proposed framework considers the intent and target of an attacker.

In a forensic examination of the Stuxnet malware [7] that affected uranium enrichment centrifuges, it was highlighted that the attack did not just target the vulnerabilities of the control systems in use, it also targeted the

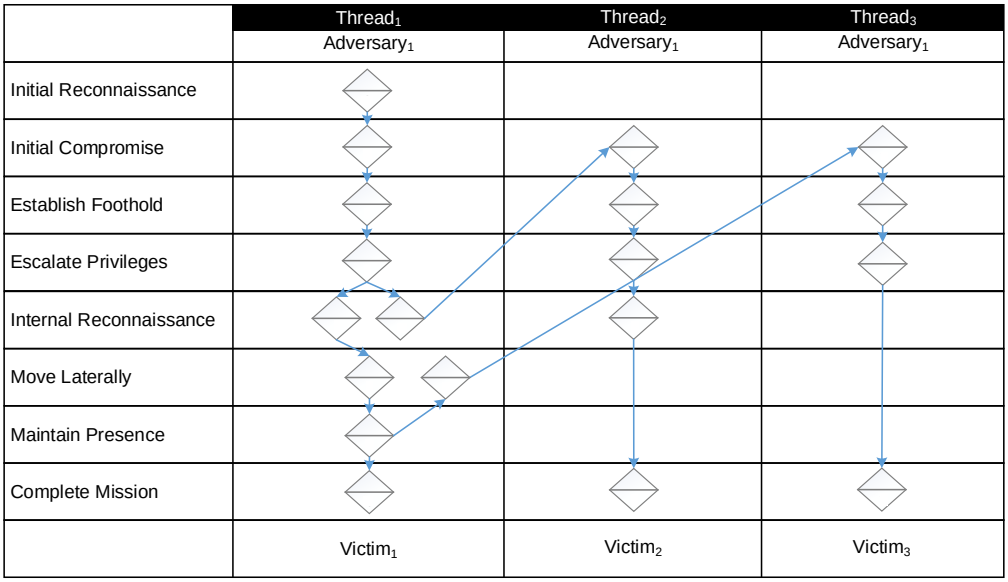

Figure 6: Activity Threads [19]

process parameters in order to create an effect in the physical world. The analysis highlighted that unlike cyber attacks on IT systems, cyber-physical attacks involve the use of IT systems to spread malware and the manipulation of ICS elements to influence the process under control that results in damage to industrial equipment. This highlights the interdependencies of the process and the control systems in use, and how one cannot be considered in isolation from the other. Many industrial facilities utilise simulation tools to model and predict the operations of the processes under control within an ICS. This forms an essential part of the operations of the facility. These models also offer the possibility to test boundary conditions of process variable and determine which ones, if maliciously manipulated, could introduce misbehaviour within the industrial process [8].

Most simulations are focused on a model of the control strategy for the process and ensure the coherence of the overall plantwide process control [26]. However, if conditions outside of this expected system state are introduced, unanticipated consequences may be observed. For example, a change in input flow into a recycle loop can result a 'snowball effect' [27] with outputs increasing by such a significant level that it leads to states whereby an

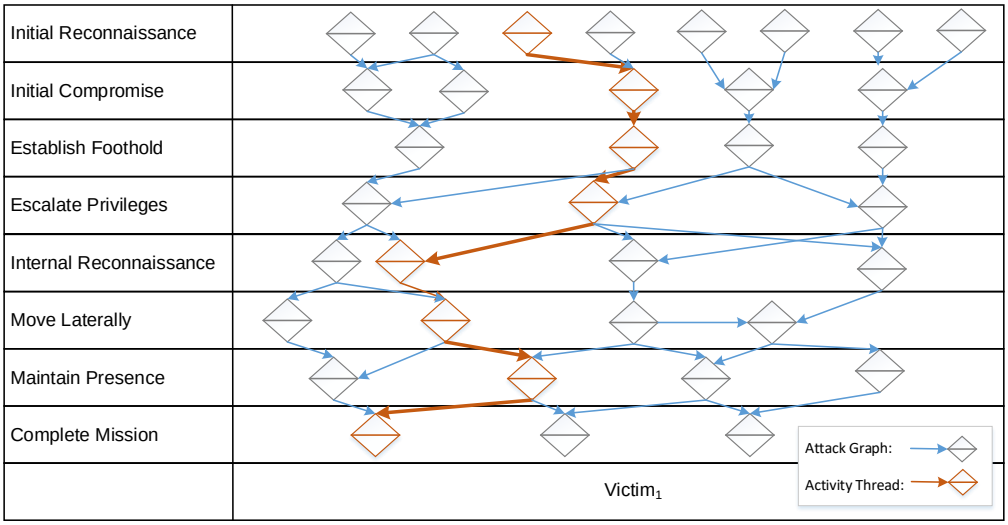

Figure 7: Activity-Attack Graph [19]

entire plant may have to be shutdown in order to rectify the situation. This demonstrates if the control equipment responsible for the input flow could be maliciously manipulated, the impact on the plant could be significant. The control device therefore becomes a key asset to defend, as an attacker with knowledge of the industrial process under control may also determine the efficacy of the device as a target [8]. Such semantic attacks can lead to long-term degradation of product or services that impede on the effectiveness and profitability of the operation.

Once the key vulnerable processes are defined, a further analysis of the feasibility of interfering with the control elements that are used to manage the parameters of the process, and highlight those that require remedial or protective measures to prevent the occurrence of such misuse. One means to identify areas of vulnerability that are potentially attractive to an antagonistic actor is the CARVER Matrix [20].

The US Department of Defense use the CARVER assessment method to determine criticality and vulnerability in enemy infrastructures. CARVER is a mnemonic for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognisability. The method focuses on an adversary's perspective of the infrastructure to enable an analysis of the weaknesses of a target, or the means by which its operations can be manipulated by an attacker [20].

In this manner, the capabilities of several threat actors can be considered. The output of the CARVER assessment is a critical-asset list that defines a prioritised set of assets that are of value to an attacker based on their importance, whereby the asset's incapacitation or destruction would have a serious impact on the military operation or facility. The use of CARVER matrices to consider threats to critical national infrastructure by civilian agencies when preparing for terrorist attacks is emerging, as it allows organisations to consider the relative desirability of targets, although its use has been limited to the assessment of physical assets [28].

Criticality *describes the level of importance the target has and its relative value to an attacker in order to achieve a desired outcome, usually a denial or degradation in the ability of a target to function.*

Accessibility *is an assessment of how an attacker could reach an asset and the complexity of reaching the desired target.*

Recuperability *considers the time and resources required to repair or replace the target, or whether viable alternatives exist.*

Vulnerability *is a measure of the ability of attackers to deny or destroy the targeted asset.*

Effect *articulates the impact of the loss or degradation of the target.*

Recognisability *is the extent to which a critical asset can be recognised by an attacker, whether this be an understanding of its existence through to knowing the detail of its location and configuration.*

Each of the categories of the CARVER acronym are assessed for an asset, using guidelines for a subjective assessment of the ratings, based on consistent criteria described at the initiation of the analysis [29]. CARVER has a standard set of criteria based on physical assets that have been refocused for ICS triage, that will allow an ICS operator to determine their level of exposure. The example in Table 3 illustrates how criticality is typically considered using in the CARVER method:

Each of six domains of CARVER are considered in an unweighted assessment, with the overall measure of their exposure based on a simple arithmetic addition of the six values applied. Using the criticality criteria above we can see how, if the processes of an industrial or critical infrastructure facility were considered, the impact of their loss would become readily apparent. Take, for example, a water supply utility [30] that takes its supplies from local rivers, treats the water to remove impurities using standard control technology, maintains a four-day storage capacity of treated water an distributes to

Criticality Criteria	**Score Rating**
Immediate termination of outcome; target cannot function without it	9-10
Loss would reduce operational performance considerably, ot two-thirds reduction in outcome	7-8
Loss would reduce operational performance, or one-third reduction in outcome	5-6
Loss may reduce operational performance, or 10 percent reduction in outcome	3-4
No significant effect on outcome	1-2

Table 1: A CARVER criticality assessment using standard criteria.

a local population via proprietary control technology. A CARVER analysis of the processes may result in the assessment described in Table 2.

Process Name	**C**	**A**	**R**	**V**	**E**	**R**	**Total**
Collection of water from rivers	7	4	3	5	7	5	31
Treatment of water	7	8	8	7	8	8	46
Storage of treated water	9	5	6	5	8	5	38
Distribution of water	8	7	6	5	8	3	37

Table 2: An example completed CARVER matrix for a water utility.

The storage of treated water appears a higher priority based on its criticality, but the lower criticality of the treatment of water is amplified by its apparent ease of access and use of standard technology that requires little industry-specific expertise to understand. This triage process allows the processes at the highest risk of being compromised to be addressed first.

Once the critical processes have been identified, the same approach can be used to identify the control devices that manage and automate them. In this manner, the scope of the analysis is immediately constrained to those systems that support the vital operational processes and provides a necessary triage. The CARVER method allows for existing, proven security methods to be brought together in a complementary framework that allows the various facets of the denial or degradation of an industrial control element to be consistently evaluated. By analysing the control logic within the device it is possible to determine which of the individual control elements, or the

interactions between elements, are responsible for the key aspects of the process under control. Such analysis allows an assessment of the ability of the process to withstand variations in conditions and data during its lifetime. This measure of robustness allows for the consequences of loss to be assessed [31].

The criticality of a device depends upon its involvement with a key process and whether or not it executes process logic or utilises process variables. Either can be manipulated to result in adverse effects on the process. These impacts can be assessed in two ways; firstly using safety analysis data, secondly using plant simulation data.

The Hazard and Operability (HAZOP) method is probably the most commonly used hazards analysis approach in industry [32]. Its widespread use and acceptance has led to a large number of practitioners and supporting service providers. The method divides systems under analysis into nodes, each of which representing a section of the process that undergoes a significant change or transformation. Examples of nodes include pumps, reactors, heat exchangers etc. This information is generally extracted from Piping and Instrumentation Diagrams (P&ID) [32]. The size of a node is a subjective decision based on the nature of the industrial process and may group devices or system elements together in order to consider an overall process change holistically. The groupings used for safety purposes are appropriate for antagonistic cyber analysis purposes as they describe malfunctions, and allow an assessment of impact and criticality should such conditions be wilfully caused.

A HAZOP analysis follows a consistent process whereby a system node is selected and its purpose and safe limits defined. Next, one of a set of *process guidewords* are selected, such as high flow, low/no flow, reverse flow, misdirected flow, high pressure, high temperature, polymerisation, wrong composition etc., that describe the effect that should be considered, and hazards and their causes are identified as a result. For each hazard, the process considers how it will be recognised should it occur, and an estimation of the consequences is reached. A set of safeguard requirements are then defined, as is the estimated frequency of the hazard's occurrence. Finally, the hazards are ranked and a set of findings and recommendations is produced.

HAZOP analyses drive a rigorous assessment of the impact of undesirable events on a process, decomposing to a detailed level. Their availability as a mechanism to assess criticality provides a rich dataset on which to base triage decisions. Where this data is not available, or when it has not covered

sufficient breadth for cyber purposes, plantwide simulations used to model the behaviour of the processes under control can be considered as a basis for study. A study of a Vinyl Acetate Monomer (VAM) process [33] assessed the vulnerabilities using an impact vocabulary that resembled a subset of the HAZOP guidewords. The full use of the HAZOP vocabulary, however, offers a structure by which the inputs, outputs, reaction vessels etc. of an industrial facility can be analysed, using the simulation to visualise and quantify the impact. Modification of the simulation to introduce financial variables will also allow the monetary impact of manipulation to be quantified.

Once the key processes have been determined, the ICS control devices that control the logic and variable used in the vulnerable process steps can be further analysed. Within control systems, disturbances in the process result in changes to process variables (PV) and represent the value sampled for control. The measurement of the PV for the purposes of process control is described as the Controlled Variable (CV), which is provided by a Primary Element such as a sensor. The CV is compared to a setpoint within the controller, generating an error, 'e', representing the deviation from the desired state. Based on this data the controller determines the necessary corrective action, represented as a Manipulated Variable (mv) that drives the behaviour of Final Control Elements such as a valve, that manipulate the mass or energy entering the process. Those control devices that act upon CV and provide logic to drive mv in the vulnerable process steps are deemed most critical [34].

In order for a cyber attack to be successful, the targeted control device must be accessible. Activity Threads [19] provide a formal way of representing the routes to a targeted control element. These are used to allow an assessment of their ease of use.

A set of CARVER accessibility criteria, modified for applicability to ICS triage, is described below. As with all of the CARVER factors described in this process, they provide guidelines to shape the consistency of the assessor's thinking, but support a subjective measure that can be derived in relatively short timescales. The accessibility criteria, modified from the original process that focusses purely on physical access to a target, guides the assessor to consider the ease with which an attacker might gain access to a critical system of device, and the likelihood of existing security mechanisms detecting such an event.

Recuperability is a measure of the control system element's ability to be replaced or repaired, and is a factor of the processes and procedures in

Accessibility Criteria	**Score Rating**
Remote or insider access with no means of identifying the attacker	9-10
Remote or insider access with limited of identifying the attacker	7-8
Remote or insider access is possible with limited auditing and logging	5-6
Remote or insider access is possible with extensive auditing and logging	3-4
Remote or insider access is extremely difficulty and will be identified	1-2

Table 3: CARVER accessibility criteria modified for ICS cyber security assessment.

place to provide a working alternative to the original device. This includes not only the replacement of the physical device, but the ability to load and execute a verified copy of the configuration necessary to operate the process. The recuperability measure can, if necessary, be tailored to the specifics of the industry under analysis. Standard CARVER recuperability criteria is applicable to ICS, and is described below. It guides the assessor to determine how long it would take to remediate the loss of a critical system or device.

Recuperability Criteria	**Score Rating**
Replacement, repair, or substitution requires 1 month or more	9-10
Replacement, repair, or substitution requires 1 week to 1 month	7-8
Replacement, repair, or substitution requires 72 hours to 1 week	5-6
Replacement, repair, or substitution requires 24 to 72 hours	3-4
Same-day replacement, repair, or substitution	1-2

Table 4: Standard CARVER recuperability criteria.

The vulnerability of a control device can depend on a number of factors. Common Vulnerabilities and Exposures (CVE) databases provide a library of known issues with control devices that can support an initial triage of potential avenues for exploitation. A modified set of accessibility criteria

that considers the capability of an antagonist is described below in order to provide accommodation for industrial equipment.

Vulnerability Criteria	**Score Rating**
Requires no industrial expertise; uses open source tools	9-10
Requires limited industrial expertise; uses open source tools	7-8
Requires extensive expertise; uses open source tools	5-6
Requires extensive industrial expertise and custom tools	3-4
Requires detailed knowledge of industrial facility and custom tools	1-2

Table 5: CARVER vulnerability criteria modified for ICS cyber security assessment.

The effect of any cyber attack must be considered in the context of the process and the physical elements involved. This is a factor of the simulation and safety documentation review conducted in the *criticality* step of the CARVER method, and is reviewed based on the following criteria, modified for a critical infrastructure facility:

Effect Criteria	**Score Rating**
Large-scale impact on services and revenues; noticeable to public	9-10
Limited impact on services and revenues; noticeable to public	7-8
Minor impact on services; minor impact on revenues; noticeable to public	5-6
Minor impact on services; minor impact on revenues; public unaware	3-4
Minor impact on services; no impact on revenues; public unaware	1-2

Table 6: CARVER effect criteria modified for ICS cyber security assessment.

In order for an attack to be enacted upon a device it is necessary for the threat actor to be aware of its existence and be able to identify it within the control network. In order to assess the risk of knowledge of existence, it should be ascertained how much of the control system architecture has been made available on open source resources such as websites, and how much is

freely discussed in communications by members of the facility's supply chain or maintenance service? The risk of identification of the device once on the control network is dependent on the control environment's ability to identify device enumeration behaviours, and are dependent upon a knowledge of the control network's traffic profile [35, 36].

A modified set of accessibility criteria is described below:

Recognisability Criteria	**Score Rating**
Requires no expertise to identify target device	9-10
Requires limited technical expertise to identify target	7-8
Requires moderate technical expertise to identify target	5-6
Requires significant technical expertise to identify target	3-4
Deception tactics deployed (honeypots etc.)	1-2

Table 7: CARVER recognisability criteria modified for ICS cyber security assessment.

The modified criteria of the CARVER matrix, *criticality*, *accessibility*, *recuperability*, *vulnerability*, *effect* and *recognisability* permits the identification and comparative ranking of ICS targets that would be attractive to a capable, antagonistic actor, in order to focus the efforts and resources of defensive activities.

For the extent of the attack options to be considered, the fourth step of the proposed framework takes each identified course of action and decompose it further. This analysis must also take into account the deployed architecture.

Fig. 8. graphically presents a single Activity Thread, derived from an Activity-Attack Graph, in a new visualisation that incorporates the deployed architecture. The usual two-dimensional representation of an Activity Thread is augmented by a third axis that shows the same attack distributed across the layers of the deployed architecture. The strength of this extension of the original model is that it allows common vulnerabilities or exploits to be considered over architectural layers, identifying areas of security weakness, or a concentration of potential attack behaviours, in individual layers. The standard Diamond Model approach to this uses a two-dimensional model, but this is again insufficient for an ICS. To allow the characteristics of a deployed ICS architecture to be accommodated, we add a third axis to architectural layers. This allows the defensive planners to review how to either detect, delay, disrupt, degrade or deceive the attacker at each layer of the architecture, considering the additional attributes defined in our extension

of the *infrastructure* and *victim* nodes of the diamond event.

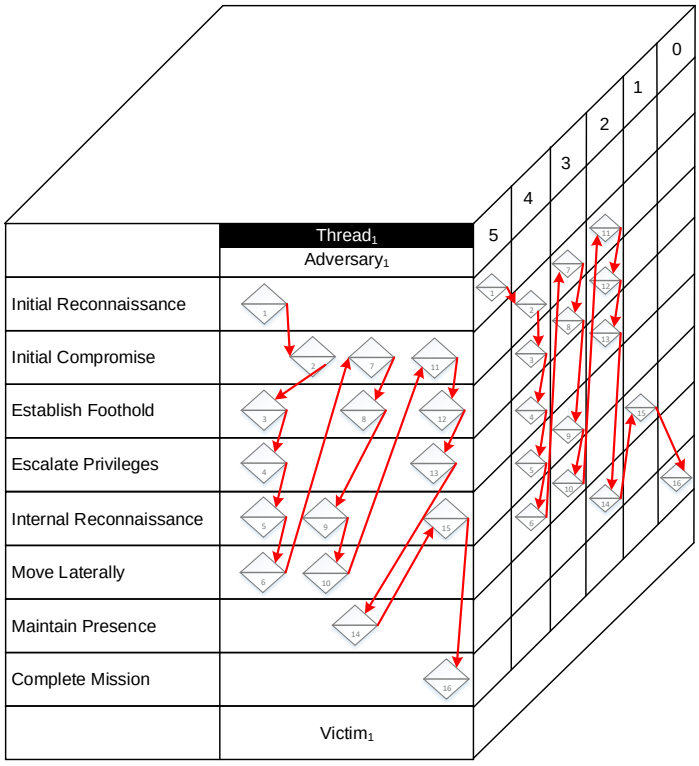

Figure 8: Extended Activity Graph, incorporating the Deployed Architecture

The example shown in Fig. 10 models the following APT attack behaviour:

1. External reconnaissance of internet boundary devices locates an internet-facing Third-party Access Server in the Enterprise Network.
2. An open, unprotected port is located and used to deliver an initial malware implant onto an unprotected File Server on the Site Business Planning and Logistics Network.
3. The malware communicates with an external command and control server and a fully-staged malware implant is deployed.
4. The malware uses a known operating system vulnerability to escalate its privileges.
5. Internal reconnaissance of the network identifies an Enterprise Resource

Planning (ERP) [37] system in the Site Business Planning and Logistics Network.
6. The malware exploits the local network infrastructure to navigate to the Manufacturing Execution System (MES) [38].
7. A beacon is deployed to the MES.
8. The beacon communicates with the command and control server via the previously compromised internet-facing server and a fully-staged implant, tailored to the device configuration, is deployed.
9. The malware performs reconnaissance of the OT network and identifies a DCS that manages processes within the plant.
10. The malware exploits the network infrastructure to reach the DCS.
11. An initial implant is deployed on the DCS that beacons to the command and control server.
12. The command and control server, communicating via the chain of compromised devices, delivers a fully-staged implant, tailored to the device configuration.
13. The malware exploits a vulnerability in the DCS's operating system to escalate its privileges.
14. The malware modifies the configuration of the DCS in order to keep its processes continually active.
15. The malware performs reconnaissance of the PLCs connected to the DCS and exfiltrates this information.
16. The malware receives instructions from the command and control server and forces a shutdown of a targeted PLC in order to stop a critical node in the plant's processing.

The results of the Attack Options Analysis feed into the final steps of the proposed framework, supporting security testing and remediation, security monitoring, and incident response planning.

For most large ICS it is not cost-effective to hold a pre-production environment for the whole facility on which to test changes [39]. This presents a challenge when testing against a representative system is required, as any use of the live environment can result in unforeseen consequences. In order to assess the levels of security available to the devices highlighted by the CARVER matrix analysis, it is necessary to define a means by which testing can be performed without risk to the operational environment. Step 5 of the process presented in this paper proposes a three-stage approach to security testing; *1. Simulated, 2. Isolated, 3. Synthesised:*

Simulated: A *process-centric* approach to security testing that uses a

simulation of the control device, modelling its logic, in order to assess the behaviours of the control strategy if the measured values, process variables, setpoints or sensor data are manipulated. The intent is to exceed normal operating parameters to test boundary conditions, and observe their impact on the process under control. The objective of this testing is not to test the security of the device, but its resilience to abnormal data and assess the error and boundary checks of the logic itself.

Isolated: A *device-centric* view of security that isolates a device identified as critical or attractive to an attacker, and assesses its inherent vulnerabilities. Preparation for isolated testing includes interrogating CVE databases to identify security testing performed elsewhere. Isolated testing should assess whether the recorded vulnerabilities are present within the device under test. However, not all vulnerabilities are identified or recorded within ICS equipment communities, so isolated testing should systematically test the device to assess its security. Techniques such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) threat modelling approach [40] allow various methods of driving a vulnerability, especially those enabled by devices that are insecure by design. Depending on the licensing of the device, techniques such as fuzzing may also be adopted.

Synthesised: An *integration-centric* set of test scenarios that assesses any vulnerabilities introduced as a consequence of the integration of critical or attractive ICS devices and components. A synthetic environment should be created as a cyber testbed to assess the device or interrelated devices in an architecturally representative environment that takes the output from the *simulated* and *isolated* stages to produce the requirements for testing at the synthesised stage. This allows the human aspect of control systems to be considered, as the testbed permits operational procedures to introduced to assess the operator's response to various situations and industrial process conditions. It also offers the additional benefit of supporting *red teams* to further analyse the attack options available to an antagonist.

As the stages of the triage process iterate, the results feedback into the ongoing analysis of the *Deployed Architecture*, *Antagonistic Target Determination*, and *Attack Options Analysis* steps, allowing remedial means to address security vulnerabilities of be assessed. It also drives the development of *Security Monitoring* strategies and *Incident Response Plans*.

Many older ICS devices are inherently insecure [39] and hardening may not be viable. At this point the defensive analysis must move from the

consideration of protection to that of active defence.

	DETECT	DENY	DISRUPT	DEGRADE	DECEIVE
Initial Reconnaissance	Web Analytics	Traffic Filtering			Fake Postings
Initial Compromise	NIDS User Education	Firewalls Anti-virus	Email Filter		Respond email out-of-office
Establish Foothold	HIDS	Traffic Filtering		Email Queuing	
Escalate Privileges		Patching	Patching		
Internal Reconnaissance	NIDS	Segmentation	Segmentation		
Move Laterally	NIDS	Whitelisting	NIPS		
Maintain Presence	HIDS			Traffic Throttling	
Complete Mission	Proxy Detection	All of above			Honeypot

Figure 9: The Diamond Model *Course of Action Matrix* integrated with the Mandiant Attack Lifecycle

A Course of Action (COA) Matrix [19] (Fig. 9) is developed from the Activity Threads and Activity-Attack Graphs an determines how to detect, deny, disrupt, degrade or deceive an attacker, as well as assisting in the analysis of where sensors should be deployed to identify antagonistic behaviours.

Hardening of devices, or strengthening the perimeter of a networked system, are essential steps toward defending an ICS from malicious activity. However, protective measures only serve to reduce the attack possibilities. When dealing with an intelligent, adaptive adversary, it is necessary to consider defensive plans to support any intrusion to allow in incident responders to anticipate the antagonists next steps. The use of Activity-Attack Graphs and COA matrices [19] considers the options available to an attacker, and describes the characteristics of each attack event using a diamond model representation, developing a set of 'competing hypotheses' [41]. This provides a basis to build an incident response 'playbook' that can be iteratively improved through table-top exercising and determine the most efficient means to deny the attacker access to the critical system assets.

4. Evaluation

For evaluation purposes, elements of the process were used in a cyber defence exercise (CDX) [42] incorporating ICS devices and involving over 500 people. As the simulation steps of the process have been demonstrated by the likes of Krotofil et al [33, 8], and require detailed process engineering specialisms, recreating these experiments was deemed unnecessary. Isolated testing of ICS devices has been widely acknowledged as a viable means of assessing vulnerabilities of individual ICS devices [43, 44, 45], and again it would not have enhanced the evaluation of the framework by repeating analyses undertaken elsewhere. The CDX, however, provided a means by which the synthesised elements of the process could be evaluated, as well as simulating antagonistic actions against an ICS. During the CDX it was observed that the use of the CARVER Matrix, with the modified assessment criteria described in this paper, identified critical systems to the continued operations of ICS facilities. However, this was initially limited to systems that provided operational functionality, as opposed to technical infrastructure systems such as domain controllers etc. The Diamond Model successfully tracked antagonistic events, using COA Matrices to determine multiple attack options, and demonstrated how analysis of Activity Thread models (a vertical analysis of the model) identified attacker progress through the networks being defended. Similarly, the horizontal analysis of the Activity Models and Activity-Attack Graphs identified common attack techniques across target networks, supporting the sharing of threat intelligence across Blue Teams. This did not prevent all Red Team activities, as systems were still compromised, but the freedom of Red Teams actions was limited to systems not assessed as critical. Red Team progress toward these systems was observed to be slower than towards non-critical systems that had not been proactively hardended, with an increased deployment of network and host sensors.

However, whilst the techniques used in the CDX demonstrated their effectiveness, they were largely paper-based, and required a significant investment of resources and effort. As the CDX progressed, the manual maintenance of paper-based data repositories became an increasing drain on Blue Team resources, suggesting that support tools would be necessary to implement the triage process at scale.

In summary, of the eight questions posed that this framework should address, Table 8 describes how the various components described in this paper interact to provide a coherent model for triaging ICS.

Question	Framework Components	Comments
1. Which devices are attractive to an attacker?	CARVER Matrix	The CARVER model supports the assessment of devices that would have the most significant impact on an ICS facility, and therefore those most attractive to a capable APT actor.
2. Can we better protect these devices?	Process simulation, device testing, synthetic environments	Process simulation identifies process variable vulnerabilities, which subsequently drives the isolated and integrated security testing of the devices responsible for using these variables.
3. What routes exist to these devices?	Activity Threads, Activity-Attack Graphs, Extended Activity Graphs, COA Matrix	The modelling of event threads and graphs supports the assessment of routes towards the identified critical devices.
4. What events would occur in an attempt to access and manipulate these devices?	Activity Threads, Activity-Attack Graphs, Extended Activity Graphs	The same event threads and graphs that determine the viable route toward a critical device are also used to determine the antagonistic events that would occur as as a result of an attack.
5. Where can we deploy sensors to detect these events?	Security monitoring and incident response planning	The positioning of sensors and IDS would be guided by the event threads and graphs. The responses to such event detection would then form the basis of an incident response plan.
6. How will we determine which of the alternate routes to a device are being used by an attacker?	COA Matrix	The sensor and IDS deployment would be based on the possible routes to critical devices. Any alerts would be cross-referenced to the COA Matrix to assess which of the many possible COAs is likely to be followed.
7. How can we predict an attackers next activity?	Activity Threads, Activity-Attack Graphs, Extended Activity Graphs, COA Matrix	With the possible COAs established, the event threads and graphs can be used to assess where along the attack path the antagonist is currently positioned, and therefore which steps must be achieved before the critical device is compromised.
8. What does our incident response plan need to describe and test in order to mitigate residual risks identified in the analysis??	CARVER, Process simulation, device testing, synthetic environments, security monitoring and incident response planning	The CARVER Matrix will highlight the initial attractiveness of a system or device, and simulation and testing will determine the extent of the associated risks. This will shape the security monitoring posture and incident response plans based on the ascertained residual risk.

Table 8: ICS Triage Framework mapped to the questions posed

5. Conclusions

The triage framework presented in this paper provides a framework to assess the attractiveness and criticality of ICS devices that underpin industrial processes. As a validated dataset describing the nature of cyber attacks on ICS is unavailable, it is based on subjective assessment of likely antagonistic targets. However, the use of safety data and simulations to drive the criticality assessment of key processes focuses on their impact on the industrial facility's ability to operate, and is based on a proven military and counter-terrorism methodology, extended for ICS. This drives the identification of those ICS devices responsible for the critical data measurements, calculations and control element manipulations that could be altered to achieve antagonistic aims, and therefore which should be triaged for immediate security testing and remediation. The approach to testing, focusing on non-destructive means that do not require access to the production environment, does not expose the ICS operator to risks that arise as a consequence of

unintended consequences of security activities.

The framework also accepts that whilst we might define the attractiveness of a target, and identify the many routes towards it for exploitation, we cannot know *a priori* which precise route the attacker will take, or how his behaviours will change based on our defensive actions. By modelling the many courses of action available to an antagonist and overlaying this onto the deployed architecture we can determine the characteristics of malicious behaviour in each segment or layer, and define the necessary signatures or heuristics by which our sensors can identify the attack. We are also able to provide security responders with a pre-incident assessment of the courses of action available to an attacker, to assist in preventing them from reaching or affecting the devices critical to the key processes of the industrial facility.

The triage framework is extendible to support synthetic environments to drive game theoretic and red/blue team exercises to better understand attacker option without subjecting the operational environment to the risks of penetration testing. This would improve the overall attack dataset for ongoing risk analysis.

The proposed framework, whilst providing a mechanism to focus security efforts and expenditure, still requires significant analysis resources to develop an initial understanding of the likely targets for an antagonist. For the framework to be feasible for large ICS installations the required timescales and manpower must be reduced in order for it to be cost-effective. Further work in this area is identified as the development of software tools to reduce the resources and timescale required, as well as expanding the use of safety data to more rapidly inform the analysis of the impact of malicious manipulation of ICS devices. Finally, the data generated as a result of the process should be assessed for its viability to feed cyber attack risk models.

References

[1] ISA. NIST Cybersecurity Framework - ISA99 Response to Request for Information, April 2013.

[2] Rafael Ramos Regis Barbosa. *Anomaly detection in SCADA systems: a network based approach*. University of Twente, 2014.

[3] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. A taxonomy of cyber attacks on scada systems. In *Internet of things (iThings/CPSCom),*

2011 international conference on and 4th international conference on cyber, physical and social computing, pages 380–388. IEEE, 2011.

[4] Brendan Galloway and Gerhard P Hancke. Introduction to industrial control networks. *Communications Surveys & Tutorials, IEEE*, 15(2):860–880, 2013.

[5] A Pauna, K Moulinos, M Lakka, J May, and T Tryfonas. Can we learn from scada security incidents? *White Paper, European Union Agency for Network and Information Security, Heraklion, Crete, Greece*, 2013.

[6] Matthew Luallen. Breaches on the rise in control systems: A sans survey. April 2014.

[7] Ralph Langner. To kill a centrifuge. *Langner Group*, 2013.

[8] Marina Krotofil and Jason Larsen. Rocking the pocket book: Hacking chemical plants. 2015.

[9] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. Scada security in the light of cyber-warfare. *Computers & Security*, 31(4):418–436, 2012.

[10] Eric Byres. Using ansi/isa-99 standards to improve control system security. The Industrial Ethernet Book, 2014.

[11] Pierre Kobes. Security levels in isa-99 / iec 62443. Online, 2012.

[12] CPNI. Cyber security assessments of industrial control systems. Online, 2011.

[13] J Mitchell, C Clarke, J Shaffer, J Su, P Chen, S Kuroda, S Smith, and B Savaris. Global industrial automation. Online, August 2012.

[14] ICS-CERT. Ics-cert year in review - 2012. Online, 2012.

[15] ICS-CERT. Ics-cert monitor november/december 2015. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERTJanuary 2016.

[16] Lloyds and The University of Cambridge Centre for Risk Studies. Business blackout: The insurance implications of a cyber attack on the us power grid. www.lloyds.com/ /media/files/news2015.

[17] NERC. High-impact, low-frequency event risk to the north american bulk power system. *A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energys November 2009 Workshop*, 2010.

[18] Allan Cook, Richard Smith, Leandros Maglaras, and Helge Janicke. Measuring the risk of cyber attack in industrial control systems. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR 2016)*, 2016.

[19] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz. The diamond model of intrusion analysis. Technical report, DTIC Document, 2013.

[20] Christopher M Schnaubelt, Eric B Larson, and Matthew E Boyer. *Vulnerability Assessment Method Pocket Guide*. RAND Corporation, 2014.

[21] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for scada systems. *computers & security*, 56:1–27, 2016.

[22] Mandiant Intelligence Center. Apt1: Exposing one of chinas cyber espionage units. *Mandian. com*, 2013.

[23] C Velazquez. Detecting and preventing attacks earlier in the kill chain. *Sans Institute*, 2015.

[24] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1:80, 2011.

[25] Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A Johnston, Sabina Piyevsky, Mark Schillace, Gregory Wilcox, Dan Zaniewski, and S Zuponcic. Converged plantwide ethernet (cpwe) design and implementation guide. *CISCO Systems and Rockwell Automation*, pages 252–253, 2011.

[26] Alexandre C Dimian, Costin S Bildea, and Anton A Kiss. *Integrated design and simulation of chemical processes*, volume 13. Elsevier, 2014.

[27] Sara Taborda, Diego A Muñoz, and Hernan Alvarez. Snowball effect detection and control proposal for its correction. In *Control Applications (CCA), 2016 IEEE Conference on*, pages 1173–1178. IEEE, 2016.

[28] Anna M Doro-on. *Risk Assessment and Security for Pipelines, Tunnels, and Underground Rail and Transit Operations*. CRC Press, 2014.

[29] Anna Doro-on. *Risk assessment for water infrastructure safety and security*. CRC Press, 2011.

[30] Ted G Lewis. *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons, 2014.

[31] Ralph Langner. *Robust control system networks*. Momentum Press, 2011.

[32] Ian Sutton. *Process risk and reliability management: operational integrity management*. Gulf Professional Publishing, 2014.

[33] Marina Krotofil and Alexander Isakov. Damn vulnerable chemical process. Online, Accessed 26 October 2016, 2014.

[34] Babak Rooholahi and P Lokender Reddy. Concept and application of pid control and implementation of continuous pid controller in siemens plcs. *Indian Journal of Science and Technology*, 8(35):1, 2015.

[35] Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras. Towards periodicity based anomaly detection in scada networks. IEEE Industrial Electronics Society, 2012.

[36] Rafael RR Barbosa, Ramin Sadre, and Aiko Pras. Difficulties in modeling scada traffic: a comparative analysis. In *Passive and Active Measurement*, pages 126–135. Springer, 2012.

[37] Turan Gonen. *Electrical Power Transmission System Engineering: Analysis and Design*. CRC Press, 2011.

[38] Christian Brecher, Simon Müller, Thomas Breitbach, and Wolfram Lohse. Viable system model for manufacturing execution systems. *Procedia CIRP*, 7:461–466, 2013.

[39] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, pages 800–82, 2011.

[40] Riccardo Scandariato, Kim Wuyts, and Wouter Joosen. A descriptive study of microsofts threat modeling technique. *Requirements Engineering*, 20(2):163–180, 2015.

[41] Craig S Fleisher and Babette E Bensoussan. *Business and competitive analysis: effective application of new and classic methods*. FT Press, 2015.

[42] Cyber defence exercise, July 2016.

[43] Feng Xie, Yong Peng, Wei Zhao, Yang Gao, and Xuefeng Han. Evaluating industrial control devices security: Standards, technologies and challenges. In *IFIP International Conference on Computer Information Systems and Industrial Management*, pages 624–635. Springer, 2014.

[44] Xi Chen and Qi Li. Research on industrial control devices flaw discovery technology. 2015.

[45] Ali Abbasi and Majid Hashemi. Ghost in the plc: Designing an undetectable programmable logic controller rootkit via pin control attack. 2016.